

# On Markovian behaviour of $p$ -adic random dynamical systems

Sergio Albeverio

Institute of Applied Mathematics  
Bonn University, 531 55 Bonn, Germany

Matthias Gundlach

Institute for Dynamical Systems  
University of Bremen, P.O. Box 330 440, 28 334 Bremen, Germany

Andrei Khrennikov and Karl-Olof Lindahl

Department of Mathematics, Statistics and Computer Science  
Växjö University, 351 95 Växjö, Sweden

February 4, 2008

## Abstract

We study Markovian and non-Markovian behaviour of stochastic processes generated by  $p$ -adic random dynamical systems. Given a family of  $p$ -adic monomial random mappings generating a random dynamical system. Under which conditions do the orbits under such a random dynamical system form Markov chains? It is necessary that the mappings are Markov dependent. We show, however, that this is in general not sufficient. In fact, in many cases we have to require that the mappings are independent. Moreover we investigate some geometric and algebraic properties for  $p$ -adic monomial mappings as well as for the  $p$ -adic power function which are essential to the formation of attractors.  $p$ -adic random dynamical systems can be useful in so called  $p$ -adic quantum physics as well as in some cognitive models.

## 1 Introduction

In this paper the state space of a dynamical system will be the field of  $p$ -adic numbers. The  $p$ -adic numbers are basically the rational numbers together with a " $p$ -adic absolute value" whose properties differ (strongly) from the ones of the usual absolute value. The  $p$ -adic numbers were explicitly first studied by K. Hensel at the end of the nineteenth century. For a long time they were only considered as a branch of pure mathematics. However, in the last decade, there has been an increasing interest for  $p$ -adic numbers in theoretical physics and biology [1]-[19].

The theory of dynamical systems is basically concerned with the study of the long-term behavior of systems. Formally, a system has two components; 1) a *state space*  $X$  : the collection of all possible states of the system, 2) a *map*  $\psi : X \rightarrow X$  from  $X$  into itself representing the evolution of the system where the state  $x_1 = \psi x$  is taken as the state at time 1 of a system which at time 0 was in  $x$ . The state  $x_0 = x$  is called the *initial state* or the initial condition of the system. In this way a state  $x_n$  is mapped into the state  $x_{n+1} = \psi x_n$  where  $x_n = \psi^n x$  represents the state of the system at time  $n$  which at time 0 was in state  $x$ .

Systems like these are deterministic in the sense that given the initial state  $x$  and the map  $\psi$  one can foresee the whole future of the system which can be represented by the *orbit*,  $\{x, \psi x, \psi^2 x, \dots, \psi^n x, \dots : n \in \mathbb{Z}^+\}$ , of  $x$  under  $\psi$ . Such models may work very well for isolated systems not perturbed by noise. But in general such models are inadequate. We have to take into account some influence of noise on the system. Therefore we let the map  $\psi$  depend on time,  $n$ , and a random parameter  $\omega$  so that  $\psi = \psi(n, \omega)$ . We will study models which involve the concept of a random dynamical system. Roughly speaking, a random dynamical system is a mechanism which at each time  $n$  randomly selects a mapping  $\psi(n, \omega)$  by which a given state  $x_n$  is mapped into  $x_{n+1} = \psi(n, \omega)x_n$ . The mappings are selected from a given family  $(\psi_s)_{s \in S}$  of mappings for some index set  $S$ . Thus  $(\psi_s)_{s \in S}$  is the set of all realizable mappings. The selection mechanism is permitted to remember the choice made at time  $n$ , *i.e.* the probability of selecting the map  $\psi_s$  at time step  $n + 1$  can depend on the choice made at time  $n$ . To model the selection procedure we use another system, a metric dynamical system, see next section.

For a random dynamical system we can only predict what will *probably* happen to the system in the future. Now, suppose that we find the system in the state  $x_n$  at time  $n$ . What is the probability of observing the state  $x_{n+1}$  in the next time step? The answer to this question may depend on our knowledge of the history of the system. In this paper we investigate under what condition we do not need to know anything about its history, except possibly its initial state, to predict the probability of its future behavior. This investigation is based on the work in [26]. Systems which behave in this way, *i.e.* the future behavior is independent of the past and depends only on the present state, are called Markov processes and are more easy to handle in scientific research. This is one of the reasons why physics has developed as it has.

In the long-term behavior of a system two things may happen: 1) Almost every possible state of the system is reached from almost every initial state (ergodicity). 2) The dynamics is attracted to an attractor  $A$  of states in the sense that there is a subset,  $U$  of  $X$ , properly containing  $A$  and consisting of states which tend to  $A$  as time goes to infinity, *i.e.*  $\lim_{n \rightarrow \infty} \psi^n u \in A$  for every  $u$  belonging to  $U$ . In the random case an attractor  $A$  may depend on

the random parameter  $\omega$  so that  $A = A(\omega)$ .

In fact, dynamical systems like those studied in this paper have been proposed as models for describing some features of the thinking process, see for example [16, 17]. In these models the consciousness generates an idea  $x$  (initial state) which evolves in time under a dynamical system in the sub-conscious. This system is perturbed by noise, physical and psychological, in a random manner. The mentioned features of the thinking process including the noise are then modeled as a  $p$ -adic random dynamical system.

In such models  $p$ -adic integers are used for the coding of cognitive information. It seems that such a  $p$ -adic coding describes well the ability of cognitive systems to form associations. A  $p$ -adic integer  $x = \sum \alpha_n p^n$  where  $\alpha_n \in \{0, 1, \dots, p-1\}$  (see section 3.1), is considered as an information string  $x = (\alpha_0, \alpha_1, \dots, \alpha_n, \dots)$ ; a  $p$ -adic distance induces the following nearness on the space of such information strings:  $x = (\alpha_j)$  and  $y = (\beta_j)$  are close if and only if  $\alpha_0 = \beta_0, \dots, \alpha_N = \beta_N$  and  $\alpha_{N+1} \neq \beta_{N+1}$  for a sufficiently large  $N$ . Thus there is a hierarchical structure between digits  $\alpha_0, \alpha_1, \dots$  which are used for the coding of an idea  $x = (\alpha_j)$ . This structure gives identification of ideas via blocks of associations  $b_0 = (\alpha_0)$ , or  $b_1 = (\alpha_0, \alpha_1)$  or  $b_2 = (\alpha_0, \alpha_1, \alpha_2), \dots$

The Markov property is a very important characteristic of the process of thinking (or memory recalling, see [19]). One of the most interesting consequences of our investigations is that the process of recalling described by the random dynamical model of [17] can be both Markovian or non-Markovian depending on the choice of the initial idea  $x$  (and the prime number  $p$ ).

## 1.1 Definition of a random dynamical system

We will study random dynamical systems in the framework of Arnold, [20]. **Definition (Random dynamical system (RDS))** Let  $(X, d)$  be a metric space with a Borel  $\sigma$ -algebra. A *measurable random dynamical system*<sup>1</sup> on the measurable space  $(X, \mathcal{B})$  over a metric DS  $(\Omega, \mathcal{F}, \mathbb{P}, (\theta(t))_{t \in \mathbb{T}})$  with time  $\mathbb{T}$  is a mapping  $\varphi : \mathbb{T} \times \Omega \times X \rightarrow X$ ,  $(t, \omega, x) \mapsto \varphi(t, \omega, x)$ , with the following properties:

- (i) *Measurability*:  $\varphi$  is  $\mathcal{B}(\mathbb{T}) \otimes \mathcal{F} \otimes \mathcal{B}$ ,  $\mathcal{B}$ -measurable.
- (ii) *Cocycle property*: The mappings  $\varphi(t, \omega) := \varphi(t, \omega, \cdot) : X \rightarrow X$  form a cocycle over  $\theta$ , i.e. they satisfy  $\varphi(0, \omega) = id_X$  for all  $\omega \in \Omega$  if  $(0 \in \mathbb{T})$ , and

$$\varphi(t + s, \omega) = \varphi(t, \theta(s)\omega) \circ \varphi(s, \omega) \quad \text{for all } s, t \in \mathbb{T}, \quad \omega \in \Omega. \quad (1)$$

---

<sup>1</sup>Random dynamical system(s) are henceforth abbreviated as "RDS".

## 1.2 Generation in Discrete Time

Let the random map  $\varphi$  be a RDS with one-sided discrete time  $\mathbb{T} = \mathbb{Z}^+$ . Let us introduce the time-one mapping  $\psi(\omega) := \varphi(1, \omega)$ . The repeated application of the cocycle property forward in time gives

$$\varphi(n, \omega) = \begin{cases} \psi(\theta^{n-1}\omega) \circ \dots \circ \psi(\omega), & n \geq 1, \\ id_X, & n = 0. \end{cases} \quad (2)$$

In this way the metric DS selects a mapping  $\psi(\theta^n\omega)$ , at each time  $n$ , which takes the state  $x_n$  to the state  $x_{n+1} = \psi(\theta^n\omega)x_n$ . Thus we can write the one-sided discrete time cocycle  $\varphi(n, \omega)x$  as the "solution" of a random difference equation

$$x_{n+1} = \psi(\theta^n\omega)x_n, \quad n \geq 0, \quad x_0 = x \in X. \quad (3)$$

Conversely, given a metric DS  $\theta = (\Omega, \mathcal{F}, \mathbb{P}, (\theta(t))_{t \in \mathbb{T}})$  and family of measurable mappings  $\psi = (\psi(\omega))_{\omega \in \Omega}$  from  $X$  into itself, such that  $(\omega, x) \mapsto \psi(\omega)x$  is  $\mathcal{F} \otimes \mathcal{B}$ ,  $\mathcal{B}$ -measurable, the map  $\varphi$  defined by (2) is a measurable RDS. We say that  $\varphi$  is *generated* by  $\psi$ .

## 2 Definition of the monomial RDS

Monomial RDS are stochastic generalizations of deterministic DS of the form

$$(X, (\psi_s^n)_{n \in \mathbb{Z}^+}), \text{ where } \psi_s x = x^s, \quad s \in \mathbb{N}, \quad x \in X. \quad (4)$$

In this paper the state space  $X$  is a subset of the field of  $p$ -adic numbers<sup>2</sup>. We shall introduce perturbations of DS defined by (4). This can be done as follows. First, let  $s$  depend on chance. That is, we let  $s : \Omega \rightarrow S = \{s_1, \dots, s_r\}$  be a discrete random variable defined on a probability space  $(\Omega, \mathcal{F}, \mathbb{P})$  equipped with a measure-preserving and invertible transformation  $\theta$ . For discrete time,  $\theta$  generates a metric DS,  $\theta := (\Omega, \mathcal{F}, \mathbb{P}, (\theta^n)_{n \in \mathbb{Z}})$ . Then we let  $\theta$  describe the perturbation of the random variable  $s$  so that  $s$  will become a stochastic process. This can be modeled with a sequence  $(S_n)$ , of random variables, where

$$S_n(\omega) = s(\omega)s(\theta\omega)\dots s(\theta^{n-1}\omega).$$

The random map  $\phi : \mathbb{Z} \times \Omega \times X \rightarrow X$ , defined by

$$\phi(n, \omega)x = \begin{cases} x^{S_n(\omega)}, & n \geq 1, \\ x, & n = 0, \end{cases} \quad (5)$$

forms a monomial RDS over the metric DS  $\theta$ . Then in the sense of (3) with  $\psi(\theta^n\omega)x = x^{s(\theta^n\omega)}$  the cocycle  $\phi(n, \omega)x$  can be considered as the solution of the random difference equation

$$x_{n+1} = x_n^{s(\theta^n\omega)}, \quad n \geq 0, \quad x_0 = x \in X.$$

---

<sup>2</sup>The field of  $p$ -adic numbers will be introduced in the next section.

The mappings  $\psi(\theta^n \omega)$  can be generated by a Markov shift in the following way. Let  $S = \{s_1, \dots, s_r\} \subset \mathbb{N}$  be the state space of the random variable  $s$  which we now want to define. For this purpose we form the product space  $S^{\mathbb{N}} = \{\omega = (\omega_0, \omega_1, \dots) : \omega_i \in S\}$  and define the random variable  $s$  as the coordinate map  $s : S^{\mathbb{N}} \rightarrow S, \omega \mapsto \omega_0$ . Then the Markov shift  $\theta = (S^{\mathbb{N}}, \mathcal{F}(S^{\mathbb{N}}), \mathbb{P}, (\theta^n)_{n \in \mathbb{N}})$  over  $S^{\mathbb{N}}$  with transition matrix  $P$ , generates a family  $(s(\theta^n \cdot))_{n \in \mathbb{N}}$  of random variables (coordinate mappings) by the relation

$$s(\theta^n \omega) = \omega_n. \quad (6)$$

Then we can consider the Markov shift  $\theta$  as a mechanism which selects mappings from the family  $\psi = (\psi_{s_1}, \dots, \psi_{s_r})$  of monomial mappings where  $\psi_{s_i} x = x^{s_i}$  and  $s_i \in S$ . Moreover, by the Markov property of the Markov shift, the random variables (6) form a Markov process. In this way the mappings  $(\psi(\theta^n \omega))_{n \in \mathbb{Z}^+}$  are Markov dependent. Thus, the role of  $S$  is to specify the realizable mappings. The Markov shift relates their dependence.

### 3 State space analysis

In order to investigate the stochastic properties of a RDS  $\phi$  of the form (5) over a Markov shift  $\theta$ , we first have to know something about the state space  $X$  of  $p$ -adic numbers and especially the properties of monomial mappings on  $X$ . The main consequence of this section is that the set of roots of unity,  $\Gamma_p$ , in  $\mathbb{Q}_p$  is an attractor for RDS  $\phi$  and that  $\Gamma_p$  is isomorphic to the multiplicative group in the residue class modulo  $p$ .

#### 3.1 $p$ -adic numbers

By the fundamental theorem of arithmetics every rational number  $x \in \mathbb{Q}$  can be written as

$$x = p^{\text{ord}_p(x)} \frac{a}{b}, \quad p \nmid ab,$$

for every prime number  $p$ . Then every prime number  $p$  induces a  $p$ -adic valuation  $|\cdot|_p$  on  $\mathbb{Q}$ ;  $|x|_p = p^{-\text{ord}_p(x)}$ , with the following properties 1)  $|x|_p = 0$  if and only if  $x = 0$ ; 2)  $|xy|_p = |x|_p |y|_p$  for every  $x, y \in \mathbb{Q}$ ; 3)  $|x + y|_p \leq \max\{|x|_p, |y|_p\}$  for every  $x, y \in \mathbb{Q}$  with equality when  $|x|_p \neq |y|_p$ . Property 3) is stronger than the "usual" triangle inequality and is called the *strong triangle inequality*. For a prime number  $p$  the  $p$ -adic valuation induces a metric  $d_p$  on  $\mathbb{Q}$  defined by  $d_p(x, y) = |x - y|_p$ . But the metric space  $(\mathbb{Q}, d_p)$  is not complete. The completion of  $\mathbb{Q}$  with respect to  $d_p$  constitutes the field of  $p$ -adic numbers which we denote by  $\mathbb{Q}_p$ . It turns out that we can represent  $\mathbb{Q}_p$  as the family of all formal sums according to

$$\mathbb{Q}_p = \{x = \sum_{n=N}^{\infty} a_n p^n : a_n \in \{0, \dots, p-1\}, \quad N = N(x) \in \mathbb{Z}\}. \quad (7)$$

Let  $x$  be a  $p$ -adic number with the expansion  $x = \sum_{n=N}^{\infty} a_n p^n$ . It can be shown, [22, 23], that  $x$  then has the valuation  $|x|_p = p^{-k}$ , if  $a_k \neq 0$  and  $a_n = 0$  for every  $n < k$ .

In other words, the integer  $k$  ( $\geq N$ ) represents the first non-zero term in the  $p$ -adic expansion (7) of  $x$ . Hence, we need not in general know every term in the sum (7) to find the valuation of a  $p$ -adic number. We compare this with the valuation on the real numbers, the absolute value, where we have to know the decimal expansion with infinite precision.

The  $p$ -adic integers, which we denote by  $\mathbb{Z}_p$ , are  $p$ -adic numbers of the form:  $\mathbb{Z}_p = \{x = \sum_{n=0}^{\infty} a_n p^n : a_n \in \{0, \dots, p-1\}\}$ . Hence the  $p$ -adic integers coincide with the unit disk,  $B_1(0)$ . In what follows we let  $S_1(0)$  denote the unit sphere.

It is often useful to consider cosets in  $\mathbb{Z}_p$ . Let us form the multiplicative coset  $p\mathbb{Z}_p = \{px : x \in \mathbb{Z}_p\}$ . Then  $p\mathbb{Z}_p$  is a maximal ideal (in fact also a prime ideal) in  $\mathbb{Z}_p$ . Let us therefore form the quotient field  $\mathbb{Z}_p/p\mathbb{Z}_p$  consisting of  $p$  additive cosets:  $p\mathbb{Z}_p, 1+p\mathbb{Z}_p, \dots, p-1+p\mathbb{Z}_p$ , isomorphic to  $\mathbb{F}_p$ ; the residue class modulo  $p$ .

**Remark 1** There is a correspondence between balls and cosets in  $\mathbb{Z}_p$  ( $\mathbb{Q}_p$ ) since  $i + p\mathbb{Z}_p = \{x \in \mathbb{Z}_p : a_0 = i\} = B_{1/p}(i)$ . Moreover two elements  $x$  and  $y$  belongs to same coset,  $i + p\mathbb{Z}_p$ , if and only if  $|x - y|_p \leq 1/p$ .

### 3.2 Fundamental properties of monomial mappings

The following lemma reveals some important properties of monomial mappings  $\psi_s$ ,

$$\psi_s : \mathbb{Q}_p \rightarrow \mathbb{Q}_p, \quad x \mapsto x^s, \quad s \in \mathbb{N},$$

on the field of  $p$ -adic numbers.

**Lemma 3.1** *Let  $\gamma \in S_1(0)$  and  $u \in p\mathbb{Z}_p$ . Then for all natural numbers  $n$ ,*

$$|(\gamma + u)^n - \gamma^n|_p \leq |n|_p |u|_p, \quad (8)$$

*with equality for  $p > 2$ .*

**Proof.** Let  $n = mp^d$ , where  $p$  does not divide  $m$ . Define  $g : x \mapsto x^m$ , and  $h : x \mapsto x^p$ . Then

$$\begin{aligned} |g(\gamma + u) - g(\gamma)|_p &= |(\gamma + u)^m - \gamma^m|_p = \left| \sum_{k=0}^m \binom{m}{k} \gamma^{m-k} u^k - \gamma^m \right|_p \\ &= |m\gamma^{m-1}u + o(u^2)|_p = |m|_p |u|_p |\gamma^{m-1}|_p = |u|_p, \end{aligned}$$

by the strong triangle inequality (here  $o(z)$  means terms of  $p$ -order smaller than or equal to the order of  $z$ , which here is simply all the rest of the binomial expansion). Thus the map  $g$  is an isometry. Set  $v = g(\gamma + u) - g(\gamma)$ ,

and  $y = g(\gamma)$ . The prime number  $p$  divides all the binomial coefficients  $\binom{p}{k}$  for  $1 < k < p$ , thus we have for  $p > 2$

$$|h(y + v) - h(y)|_p = |pvy^{p-1} + o(pv^2)|_p = |p|_p |v|_p = |p|_p |u|_p,$$

and for  $p = 2$  we have

$$|h(y + v) - h(y)|_p = |pvy^{p-1} + o(v^2)|_p \leq |p|_p |v|_p = |p|_p |u|_p.$$

Thus,  $d$  iterations of  $h$  give

$$|(\gamma + y)^n - \gamma^n|_p = \left| h^d(g(\gamma + u)) - h^d(g(\gamma)) \right|_p \leq |n|_p |u|_p,$$

where equality holds for  $p > 2$ .  $\square$

**Corollary 3.1** *Let  $x, y \in S_1(0)$  and suppose  $|x - y|_p < 1$ . Then for all natural numbers  $n$ ,*

$$|x^n - y^n|_p \leq |n|_p |x - y|_p, \quad (9)$$

*with equality for  $p > 2$ .*

**Proof.** By hypothesis  $x - y \in p\mathbb{Z}_p$ . Put  $x - y = u$  and  $x = \gamma$ . Then the corollary follows directly from Lemma 3.1.  $\square$

**Remark 2** The equality  $\left| \sum_{k=1}^n \binom{n}{k} y^{n-k} (x - y)^k \right|_p = |n|_p |x - y|_p$  does not always hold for  $p = 2$ ; For example  $\left| \sum_{k=1}^4 \binom{4}{k} 3^{n-k} 2^k \right|_2 < |4|_2 |2|_2$ . Hence we do not always have equality in (9) in the case that  $p = 2$ .  $\square$

Let  $s$  be a natural number divisible by  $p$ . From Corollary 3.1 we see that the corresponding monomial map  $\psi_s$  is contracting on the unit sphere  $S_1(0)$  since in this case we have  $|\psi_s x - \psi_s y|_p \leq 1/p |x - y|_p$ . We will use a special case ( $s = p$ ) to determine all possible fixed points under monomial mappings on  $\mathbb{Q}_p$ .

### 3.2.1 Fixed points and roots of unity in $\mathbb{Q}_p$

In the study of dynamical systems it is important to know the fixed points of the mappings generating the system. A point  $x$  is a *fixed point* under the monomial map  $\psi_s$  if and only if it satisfies the equation  $\psi_s x = x$ , i.e. if  $x^s = x$ . Clearly 0 is a fixed point under iterations of  $\psi_s$  for all natural numbers  $s$ . A fixed point  $x \neq 0$  under a monomial map  $\psi_s$  satisfies  $x^{s-1} = 1$  (since  $\mathbb{Q}_p$  is a field every element except 0 has a multiplicative inverse), i.e.  $x$  is a root of unity. In  $\mathbb{Q}_p$  ( $\mathbb{Z}_p$ ) there are  $p - 1$  roots of unity. One can show the existence of  $p - 1$  zeroes to the polynomial  $F(x) = x^{p-1} - 1$  by studying the monomial map  $\psi_p : x \mapsto x^p$ :

First we observe that each coset in  $\mathbb{Z}_p/p\mathbb{Z}_p$  is closed under iterations of  $\psi_p$ . This is a consequence of the fact that  $a^p \equiv a \pmod{p}$ . Moreover the condition of Corollary 3.1 is satisfied for every coset,  $i + p\mathbb{Z}_p$  where  $i \neq 0$ , see Remark 1. From this we conclude that  $\psi_p$  is a contraction on each of these cosets (as a consequence of Banach's fixed point theorem). That  $\psi_p$  is a contraction on  $p\mathbb{Z}_p = B_{1/p}(0)$  follows from the strong triangle inequality. Consequently every coset,  $i + p\mathbb{Z}_p$ , has a unique fixed point,  $\xi_i$ , such that  $\xi_i^p = \xi_i$ . And if  $i$  is different from 0 we also have that  $\xi_i^{p-1} = 1$ . This proves the existence of  $p-1$  roots of unity in  $\mathbb{Q}_p$  (in fact this is a trivial consequence of Hensel's lemma [22, 23]; however, we prefer to present a direct proof). There are no more roots of unity in  $\mathbb{Q}_p$ .

Let  $\Gamma_p$  be the set of the  $p-1$  zeroes of the polynomial  $F$  where  $F(x) = x^{p-1} - 1$  in  $\mathbb{Q}_p$ . Then  $\Gamma_p$  is closed under multiplication and isomorphic to the multiplicative group,  $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ ; let  $\xi_i$  be the root belonging to  $i + p\mathbb{Z}_p$ . Then  $\xi_i \cdot \xi_j \in i \cdot j + p\mathbb{Z}_p$  so that  $\xi_i \cdot \xi_j = \xi_{i \cdot j \bmod p}$ .

### 3.3 Continuous case-the $p$ -adic power function

We now generalize our RDS  $\phi$  to the continuous case, *i.e.* we let the random variables  $(s(\theta^n \cdot))_{\mathbb{Z}_+}$  take values in the state space  $S = \mathbb{Z}_p$ . Then we have to study properties of the  $p$ -adic power function  $x \mapsto x^a$ . This map is defined for  $x \in 1 + \mathbb{Z}_p$  and  $a \in \mathbb{Z}_p$  by

$$x^a = \sum_{n=0}^{\infty} \binom{a}{n} (x-1)^n,$$

where

$$\binom{a}{0} := 1, \quad \binom{a}{n} := \frac{a(a-1)\dots(a-n+1)}{n!}, \quad n \in \mathbb{N}.$$

Here is a result which is analogous to the one in the monomial case, with essentially the same proof as in Lemma 3.1.

**Lemma 3.2** *Let  $x \in 1 + p\mathbb{Z}_p$ . Then*

$$|x^a - 1|_p \leq |a|_p |x - 1|_p, \quad (10)$$

*holds, with equality for  $p > 2$ .*

**Proof.** Let  $a = a_0 p^d$ , where  $a_0 \in S_1(0)$ , and put  $\gamma = 1$  and  $u = x - 1$ . Define  $g: x \mapsto x^{a_0}$ , and  $h: x \mapsto x^p$ . Then

$$\begin{aligned} |g(\gamma + u) - g(\gamma)|_p &= |x^{a_0} - 1|_p = \left| \sum_{n=0}^{\infty} \binom{a_0}{n} (x-1)^n - 1 \right|_p \\ &= |a_0 u + o(u^2)|_p = |u|_p, \end{aligned}$$



by the strong triangle inequality. The rest of the proof is the same as in that of Lemma 3.1  $\square$

We see from the lemma that for every  $x \in 1 + p\mathbb{Z}_p$  the sequence  $x^{S_n(\omega)}$  converges to 1 if  $s(\theta^n \omega)$  belongs to  $p\mathbb{Z}_p$  infinitely often. This is the case when  $\mathbb{P}\{s(\omega) \in p\mathbb{Z}_p\}$  is greater than zero. To see this let us recall the concept of recurrence. Here we follow to the classical book of P.R. Halmos [24].

**Definition (Recurrent point)** Let  $(X, \mathcal{B}, \mu)$  be a finite measure space. Let  $B \in \mathcal{B}$  and let  $T$  be a measure-preserving transformation. A point  $x$  is said to be *recurrent with respect to  $B$*  if there is a natural number  $k$  for which  $T^k x \in B$ .

In the spirit of this definition we have the following famous result from ergodic theory.

**Theorem 3.1 Recurrence Theorem.** *For each  $B \in \mathcal{B}$  with  $\mu(B) > 0$  almost every point of  $B$  is recurrent with respect to  $B$ .*

The Recurrence theorem implies a stronger version of itself. In fact, for almost every  $x$  in  $B$  (with  $\mu(B) > 0$ ), there are infinitely many values of  $n$  such that  $T^n x \in B$ , see for example [24]. Let  $B = \{\omega : s(\omega) \in p\mathbb{Z}_p\}$  with  $\mathbb{P}(B) > 0$  and let  $\theta$  be the Markov (left) shift (which is measure-preserving). Then it follows from the recurrence theorem that for almost every point  $\omega$  in  $B$  there must be an arbitrarily large number of moments in time when the trajectory of the point  $\omega$  is in the set  $B$ , *i.e.* for almost every  $\omega \in B$ ,  $s(\theta^n \omega)$  belongs to  $p\mathbb{Z}_p$  infinitely often. Moreover, if  $\theta$  is ergodic, almost all points of the space enter the set  $B$ , and of course once they are in there they will return infinitely many times by the recurrence theorem. In the case that  $\theta$  is ergodic we then have that  $\{1\}$  is an attractor<sup>3</sup> for the RDS  $\phi$  if  $\mathbb{P}(s(\omega) \in p\mathbb{Z}_p) > 0$ .

**Theorem 3.2** *Let  $\theta$  be ergodic and let  $\mathbb{P}(s(\omega) \in p\mathbb{Z}_p) > 0$ . Then the set  $\{1\}$  is an attractor for the RDS  $\phi$  on  $X = 1 + p\mathbb{Z}_p$ .*

**Proof.** We show that

$$\lim_{n \rightarrow \infty} \text{dist}(\phi(n, \omega)X, \{1\}) = 0 \quad \mathbb{P} - a.e.$$

---

<sup>3</sup>See Appendix A for the definition of an attractor.

By definition

$$\begin{aligned}
\text{dist}(\phi(n, \omega)X, \{1\}) &= \sup_{x \in 1+p\mathbb{Z}_p} \inf_{z \in \{1\}} |\phi(n, \omega)x - z|_p \\
&= \sup_{x \in 1+p\mathbb{Z}_p} |\phi(n, \omega)x - 1|_p \\
&= \sup_{x \in 1+p\mathbb{Z}_p} |x^{S_n(\omega)} - 1|_p \\
&\leq \sup_{x \in 1+p\mathbb{Z}_p} |S_n(\omega)|_p |x - 1|_p \\
&= |S_n(\omega)|_p \frac{1}{p} \\
&\rightarrow 0 \quad \mathbb{P} - a.e.,
\end{aligned}$$

when  $n$  goes to infinity by Poincaré Recurrence Theorem, and the last equality holds by Lemma 3.2.  $\square$

Let us now return to the discrete case.

### 3.4 Attractors

Attractors of systems like (5) have been studied in [17] for the case that  $p$  divides at least one  $s_i \in S$ . It was shown that there are only deterministic attractors on  $\mathbb{Q}_p$ . First,  $\{0\}$  and the point at infinity,  $\{\infty\}$ , are attractors. The points attracted to these sets are  $U_{1/p}(0) = \{x \in \mathbb{Q}_p : |x|_p \leq 1/p\}$  and  $\mathbb{Q}_p \setminus \mathbb{Z}_p$  respectively. If one of the elements in the state space  $S$  of the random variable  $s$  is divisible by  $p$ , then there is one more attractor on  $\mathbb{Q}_p$ . This attractor is a subset of  $\Gamma_p$ . In [17] it was proved with the aid of Lemma 3.1 that in the case that  $p$  divides one of the numbers in  $S$ , then the points on  $S_1(0) = \{x \in \mathbb{Q}_p : |x|_p = 1\}$  are attracted to  $I_s = \psi_{s_1}^{p-1} \circ \dots \circ \psi_{s_r}^{p-1}(\Gamma_p)$ . The proof is based on the same procedure as in the proof of Theorem 3.2.

We now want to say something about the case when  $p$  does not divide any of the elements in the state space  $S$  of the random variables.

### 3.5 Random Siegel disk

Let us introduce a generalization of Siegel disks<sup>4</sup> which we call random Siegel disks. To do this we define a metric  $d$  by  $d(x, A) := \inf_{a \in A} |x - a|_p$ .

**Definition (Random Siegel disk, Maximal random Siegel disk)** Let the RDS  $\varphi$  be generated by a family  $\psi = (\psi_{s_1}, \dots, \psi_{s_r})$  of monomial mappings:  $\psi_{s_i}x = x^{s_i}$ , in the sense of section 1.2. Let  $A$  be an *invariant* set, i.e.  $\psi_{s_1} \circ \dots \circ \psi_{s_r}(A) = A$ . Let  $O$  be a subset of  $\mathbb{Q}_p$  properly containing  $A$ . Then  $O$  is said to be a *random Siegel disk* for the RDS  $\varphi$  concentrated around  $A$

---

<sup>4</sup>See for example [25].

if, for almost every  $\omega$ ,

$$d(x, A) = d(\varphi(n, \omega)x, A),$$

for every  $x \in O$  and every  $n \in \mathbb{Z}^+$ . The set  $\tilde{O} = \bigcup O$ , the union of all random Siegel disks around  $A$ , is said to be a *maximal random Siegel disk* around  $A$ . By Lemma 3.1 we obtain the following result.

**Theorem 3.3** *Let  $p > 2$ , see Lemma 3.1. Let the monomial RDS  $\phi$  be generated by a family  $\psi = (\psi_{s_1}, \dots, \psi_{s_r})$  of monomial mappings where  $\psi_{s_i}x = x^{s_i}$ . Let  $I_s = \psi_{s_1}^{p-1} \circ \dots \circ \psi_{s_r}^{p-1}(\Gamma_p)$  and suppose that  $p$  does not divide any of the  $s_i \in S$ . Then  $\mathbb{Z}_p$  is a maximal random Siegel disk concentrated around  $I_s$  for the RDS  $\phi$ .*

**Proof.** First we prove that  $S_1(0)$  is a random Siegel disk around  $I_s$ . Clearly  $I_s = \psi_{s_1}^{p-1} \circ \dots \circ \psi_{s_r}^{p-1}(\Gamma_p)$  is an invariant set. Moreover, for every  $x$  on the unit sphere  $S_1(0)$  we have by Lemma 3.1 for  $p > 2$  that

$$\begin{aligned} d(x^{S_n(\omega)}, I_s) &= \inf_{a \in I_s} |x^{S_n(\omega)} - a|_p = \inf_{a \in I_s} |x^{S_n(\omega)} - a^{S_n(\omega)}|_p \\ &= \inf_{a \in I_s} |S_n(\omega)|_p |x - a|_p = \inf_{a \in I_s} |x - a|_p = d(x, I_s), \end{aligned}$$

where the last equality holds because  $p$  does not divide any of the elements in  $S$  and therefore not a product  $S_n(\omega)$  so that  $|S_n(\omega)|_p = 1$ . Now,  $p\mathbb{Z}_p$  is also a random Siegel disk since  $x^{S_n(\omega)} \in p\mathbb{Z}_p$  for every  $n$  if  $x \in p\mathbb{Z}_p$  which implies that

$$d(x^{S_n(\omega)}, I_s) = 1 = d(x, I_s),$$

for every  $x \in p\mathbb{Z}_p$ . But  $\mathbb{Z}_p = S_1(0) \cup p\mathbb{Z}_p$  and  $|x^{S_n(\omega)} - a|_p \rightarrow \infty$  for every  $x$  outside  $\mathbb{Z}_p = B_1(0)$ . Hence  $\mathbb{Z}_p$  is maximal as required.  $\square$

## 4 Definition of Markovian dynamics

Let  $X = \Gamma_p$ . Given an initial state  $x \in X$ , our RDS defined by the random map  $\phi$ , defined by (5), over a Markov shift  $\theta$  can be considered as a  $\Gamma_p$ -valued stochastic process defined by the forward motion

$$(x^{S_n})_{n \in \mathbb{Z}^+} = (\phi(n, \cdot)x)_{n \in \mathbb{Z}^+}. \quad (11)$$

We say that a sequence  $(x^{S_n(\omega)})_{n=1}^N$  is an  $N$  step *realization* of the stochastic process (11). Then  $(x^{S_n})_{n \in \mathbb{Z}^+}$  is a stochastic process with state space  $\Gamma_p$  and transition probability  $P(x, B) = \mathbb{P}\{\omega : x^{S(\omega)} \in B\}$  (a proof is given in [20]). Thus, on  $\Gamma_p$  we have a family  $(x^{S_n})_{x \in \Gamma_p}$  of stochastic processes. We want to investigate when each process  $(x^{S_n})_{n \in \mathbb{Z}^+}$  satisfies the (weak) Markov property

$$\begin{aligned}\mathbb{P}(\phi(1+n, \omega)x &= x_{n+1} \mid \phi(n, \omega)x = x_n, \dots, \phi(1, \omega)x = x_1) \\ &= \mathbb{P}(\phi(1+n, \omega)x = x_{n+1} \mid \phi(n, \omega)x = x_n),\end{aligned}\quad (12)$$

for every sequence  $(x_i \in \Gamma_p)$  such that

$$\mathbb{P}(\phi(n, \omega)x = x_n, \dots, \phi(1, \omega)x = x_1) > 0.$$

In doing so we define *transition sets*

$$A^n(x, y) = \{\alpha = \alpha_1 \cdot \dots \cdot \alpha_n : \alpha_i \in S \text{ and } x^\alpha = y\}, \quad (13)$$

of all possible ordered products of  $n$  elements in  $S$ , taking  $x$  to  $y$  in  $n$  steps. With the aid of the transition sets (13) we can write the probability of the  $n$  step realization  $(x_i)_{i=1}^n$  as

$$\begin{aligned}\mathbb{P}(x^{S_1(\omega)} &= x_1, x^{S_2(\omega)} = x_2, \dots, x^{S_n(\omega)} = x_n) \\ &= \mathbb{P}(x^{s(\omega)} = x_1, x_1^{s(\theta\omega)} = x_2, \dots, x_{n-1}^{s(\theta^{n-1}\omega)} = x_n) \\ &= \mathbb{P}(s(\omega) \in A^1(x, x_1), \dots, s(\theta^{n-1}\omega) \in A^1(x_{n-1}, x_n)) \\ &= \mathbb{P}(\omega_0 \in A^1(x, x_1), \dots, \omega_{n-1} \in A^1(x_{n-1}, x_n)).\end{aligned}$$

On  $\Gamma_p$  the dynamics is discrete. Thus (for a sequence  $(x_i)$  where  $x_i \in \Gamma_p$ ) the weak Markov property (12) is satisfied if and only if the *Markov equation*

$$\begin{aligned}\mathbb{P}(\omega_n &\in A^1(x_n, x_{n+1}) \mid \omega_{n-1} \in A^1(x_{n-1}, x_n), \dots, \omega_0 \in A^1(x, x_1)) \\ &= \mathbb{P}(\omega_n \in A^1(x_n, x_{n+1}) \mid \omega_0 \cdot \dots \cdot \omega_{n-1} \in A^n(x, x_n)),\end{aligned}\quad (14)$$

holds true for every sequence  $(x_i \in \Gamma_p)$  such that

$$\mathbb{P}(\omega_0 \in A^1(x, x_1), \dots, \omega_n \in A^1(x_{n-1}, x_n)) > 0. \quad (15)$$

**Remark 3** Note that on the right hand side of the Markov property defined by (12) we allow dependence on the initial state  $x$ . This is in fact the *weak Markov property*, see for example [21]. Another formulation of Markovian dynamics, allowing no dependence on the past, could be: The dynamics on  $X$  is Markovian under the RDS  $\phi$  if

$$\begin{aligned}\mathbb{P}(\phi(1+n, \omega)x &= x_{n+1} \mid \phi(n, \omega)x = x_n, \dots, \phi(1, \omega)x = x_1) \\ &= \mathbb{P}\{\omega : \psi(\theta^n \omega)x_n = x_{n+1}\}.\end{aligned}$$

In this case  $\theta$  has to be a Bernoulli shift since  $\mathbb{P}\{\omega : \psi(\theta^n \omega)x_n = x_{n+1}\} = \mathbb{P}(\omega_n \in A^1(x_n, x_{n+1}))$  so that

$$\begin{aligned}\mathbb{P}(\omega_n &\in A^1(x_n, x_{n+1}) \mid \omega_{n-1} \in A^1(x_{n-1}, x_n), \dots, \omega_0 \in A^1(x, x_1)) \\ &= \mathbb{P}(\omega_n \in A^1(x_n, x_{n+1})).\end{aligned}$$

□

In what follows we consider Markovian dynamics in the framework of *weak Markov property*, namely Markov families, see [20, 21].

The family  $(x^{S_n})_{x \in \Gamma_p}$  of processes is called a *Markov family* if and only if  $(x^{S_n})_{n \in \mathbb{Z}^+}$  is a Markov process for each initial state  $x \in \Gamma_p$ . We say that the *dynamics* on  $\Gamma_p$  is *Markovian* if  $(x^{S_n})_{x \in \Gamma_p}$  is a Markov family<sup>5</sup>.

We remark that the sufficient condition for Markovian dynamics is that  $\theta$  is a Bernoulli shift.

One may ask whether this can be generalized directly to any Markov shift, *i.e.* to every stochastic matrix  $P$ . The following example illustrates that this is in fact not the case.

**Example (A non-Markovian  $p$ -adic chain)** Consider the RDS on  $\Gamma_7$ . Let  $S = \{7, 2, 3\}$  and let the elements of  $S$  be distributed by  $\pi = \frac{1}{20}(8, 9, 3)$ . The probability vector  $\pi$  is a row eigenvector of the stochastic matrix

$$P = \begin{pmatrix} \frac{1}{2} & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{3} & \frac{2}{3} & 0 \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix}.$$

Let  $\mathbb{P} = \mu_{\pi P}$  be the corresponding Markov measure. Let  $\xi$  be a primitive 6th root of unity in  $\mathbb{Q}_7$  so that  $\Gamma_7 = \{1, \xi, \xi^2, \xi^3, \xi^4, \xi^5\}$ . Note that on  $\Gamma_7$  we have that  $x^7 = x^1$  for every  $x$ . Then consider the initial state  $x_0 = \xi$  and the realization

$$(\xi^3, \xi^3, 1).$$

Then the one step transition sets, defined by (13), are  $A^1(\xi, \xi^3) = \{3\}$ ,  $A^1(\xi^3, \xi^3) = \{1\}$  and  $A^1(\xi^3, 1) = \{2\}$ . Hence the left hand side of (14) becomes

$$\mathbb{P}(\omega_2 = 2 \mid \omega_1 = 1, \omega_0 = 3) = \frac{\mathbb{P}([3, 1, 2])}{\mathbb{P}([3, 1])} = \frac{p_3 p_{31} p_{12}}{p_3 p_{31}} = p_{12} = \frac{1}{4},$$

and the right hand side with the two step transition set  $A^2(\xi, \xi^3) = \{3\}$ :

$$\begin{aligned} \mathbb{P}(\omega_2 = 2 \mid \omega_1 \cdot \omega_0 = 3) &= \frac{\mathbb{P}([3, 1, 2]) + \mathbb{P}([1, 3, 2])}{\mathbb{P}([3, 1]) + \mathbb{P}([1, 3])} \\ &= \frac{p_3 p_{31} p_{12} + p_1 p_{13} p_{32}}{p_3 p_{31} + p_1 p_{13}} = \frac{8 \frac{1}{4} \frac{1}{3} + 3 \frac{1}{3} \frac{2}{3}}{8 \frac{1}{4} + 3 \frac{1}{3}} = \frac{4}{9}. \end{aligned}$$

Thus we have found a non-Markovian  $p$ -adic chain. □

This was the counterexample but we can ask: Is there any stochastic matrix  $P$  which is not generating a Bernoulli shift and still satisfies the Markov equation (14)? And, on the contrary, are there state spaces  $\Gamma_p$  and  $S$  such that (14) implies that  $\theta$  has to be a Bernoulli shift? We will see that for some  $S$  we have to require that our Markov shift is a Bernoulli shift in order to get Markovian dynamics.

<sup>5</sup>This approach is quite natural for models of the process of thinking [16, 17, 19]. Here the choice of the initial idea  $x$  plays the crucial role.

## 5 Conditions for Markovian dynamics

In order to solve the Markov equation (14) we need to find transition sets (for possible realizations  $(x_i)_{i=1}^n$ ) defined by (13). To facilitate this procedure we take advantage of the algebraic properties of  $\Gamma_p$ . It was stated in section 3 that  $\Gamma_p$  is (algebraically) isomorphic to  $\mathbb{F}_p^*$ , the multiplicative subgroup of the residue class modulo  $p$ . Hence  $\Gamma_p$  is a cyclic group under multiplication with  $p - 1$  elements. Thus one of the roots,  $\xi$ , is a primitive  $(p - 1)th$  root of unity so that  $\Gamma_p = \{1, \xi_{p-1}, \dots, \xi_{p-1}^{p-2}\}$ . Moreover every element  $x \in \Gamma_p$  (in particular the initial state of the RDS) is generating a subgroup

$$\langle x \rangle = \{1, x, \dots, x^{k-1} : x^i \neq 1 \text{ for } 0 < i < k \text{ and } x^k = 1\},$$

with  $k$  elements. We say that  $\langle x \rangle$  is of *order*  $k$  and let  $|\langle x \rangle|$  denote the order of  $x$ . Hence an equality  $x^{ab} = x^{cd}$  can be formulated as a congruence in the sense that

$$x^{ab} = x^{cd} \Leftrightarrow ab \equiv cd \pmod{|\langle x \rangle|}. \quad (16)$$

Consequently, we can determine transition sets (13) counting modulo  $|\langle x \rangle|$ :

$$A^n(x, x^\beta) = \{\alpha = \alpha_1 \cdot \dots \cdot \alpha_n : \alpha_i \in S \text{ and } \alpha \equiv \beta \pmod{|\langle x \rangle|}\}.$$

**Remark 4** Given the initial state  $x$  the dynamics is restricted to  $\langle x \rangle$ . From (16) it follows that the dynamics on  $\langle x \rangle$  under the RDS  $\phi$  is totally described by the dynamics on  $S$  if the elements in  $S$  are considered as elements in the residue class modulo  $|\langle x \rangle|$ , which we denote by  $\mathbb{F}_{|\langle x \rangle|}$ . Therefore the properties of the long-term behaviour of the RDS on  $\Gamma_p$  depend strongly on the order of  $x$ . If the order of  $x$ ,  $|\langle x \rangle|$ , is not a prime, the residue class modulo  $|\langle x \rangle|$  contains divisors of zero, *i.e.* there are elements  $a, b \in \mathbb{F}_{|\langle x \rangle|}$  different from 0 in  $\mathbb{F}_{|\langle x \rangle|}$  such that  $ab \equiv 0 \pmod{|\langle x \rangle|}$ . Then  $x^{ab} = x^0 = 1$  which leads to trivial dynamics. For example  $2 \cdot 2 = 4$  which equals 0 in  $\mathbb{F}_4$ . But if  $|\langle x \rangle|$  is prime then  $\mathbb{F}_{|\langle x \rangle|}$  is a field. Thus  $\mathbb{F}_{|\langle x \rangle|}^* = \mathbb{F}_{|\langle x \rangle|} \setminus \{0\}$  is a group under multiplication and therefore contains no divisors of zero. Consequently, if  $|\langle x \rangle|$  is a prime number and  $S \subseteq \{1, \dots, |\langle x \rangle| - 1\}$  the dynamics is restricted to  $\langle x \rangle \setminus \{1\}$  so that the RDS can not enter the state 1. Hence, to avoid trivial dynamics we will thus assume that the order of  $x$  is a prime number <sup>6</sup> different from 2 (If  $|\langle x \rangle| = 2$ ,  $S$  will contain only one element.) and that  $S \subseteq \{1, \dots, |\langle x \rangle| - 1\}$ . Such an  $x$  exists if  $p \not\equiv 1 \pmod{4}$ ; by the theorem of Lagrange we know that  $|\langle x \rangle|$  is a divisor of  $|\Gamma_p| = p - 1$ . Since  $\Gamma_p$  is abelian the inverse of the theorem of Lagrange Theorem is also true, *i.e.* given a prime divisor  $n$  of  $p - 1$  there is a  $x \in \Gamma_p$  of order  $n$ . Now  $p - 1$  is divisible by a prime number different from 2 if  $p \not\equiv 1 \pmod{4}$ .  $\square$

---

<sup>6</sup>The case where  $|\langle x \rangle|$  is not a prime for any  $x \in \Gamma_p$  is treated in Section ??.

**Remark 5** If  $|\langle x \rangle|$  is prime and  $S \subseteq \{1, \dots, |\langle x \rangle| - 1\}$ , then all one step transition sets  $A^1(x_i, x_{i+1})$ ,  $x_j \in \Gamma_p$  are singletons. This is a direct consequence of the group property of  $\mathbb{F}_{|\langle x \rangle|}^*$ .  $\square$

Furthermore, it is clear that we only need to consider  $n$  step conditional probabilities in (14) for which  $n \geq 3$ , since (14) is always valid for  $n = 2$ . The following results describe how the Markov equation (14) is putting conditions on the entries in the transition matrix  $P$ . We shall consider the case of Markov shifts generated by transition matrices with row eigenvectors  $\pi$  where  $p_i > 0$  for all  $i \in S$ . This is not a real restriction; since otherwise no cylinder containing  $s_i$  would have positive measure. Then the state  $s_i$  might as well be deleted. As a consequence, each row and each column of  $P$  contains a positive entry.

Also note that if the columns of  $P$  are constant, then the corresponding Markov shift is just a Bernoulli shift.

**Lemma 5.1** *Let  $|\langle x \rangle|$  be a prime number,  $S \subseteq \{1, \dots, |\langle x \rangle| - 1\}$  and let  $i_1 \cdot \dots \cdot i_n, i_r \in S$  be an arbitrary ordered product. Then the  $n+1$  step realization  $(x^{i_1}, \dots, x^{i_1 \dots i_n k})$ , given the  $n$  step realization  $(x^{i_1}, \dots, x^{i_1 \dots i_n})$ , generates the Markov equation*

$$p_{i_n k} = \mathbb{P}(\omega_n = k \mid \omega_0 \cdot \dots \cdot \omega_{n-1} \in \{\alpha : \alpha \equiv i_1 \cdot \dots \cdot i_n \pmod{|\langle x \rangle|}\}),$$

*if and only if  $p_{i_1 i_2} \cdot \dots \cdot p_{i_{n-1} i_n} > 0$ .*

**Proof.** First we prove that (15) is satisfied if and only if  $p_{i_1 i_2} \cdot \dots \cdot p_{i_{n-1} i_n} > 0$ . In Remark 5 we found that one step transition sets are singletons. Therefore

$$\begin{aligned} \mathbb{P}(\omega_0 \in A^1(x, x^{i_1}), \dots, \omega_{n-1} \in A^1(x^{i_1 \dots i_{n-1}}, x^{i_1 \dots i_{n-1} i_n})) \\ = \mathbb{P}(\omega_0 = i_1, \dots, \omega_{n-1} = i_n) = p_{i_1} p_{i_1 i_2} \cdot \dots \cdot p_{i_{n-1} i_n}, \end{aligned}$$

which is greater than zero if and only if  $p_{i_1 i_2} \cdot \dots \cdot p_{i_{n-1} i_n} > 0$  (we assume that  $p_{i_1} > 0$ ). For the left hand side of (14) we obtain

$$\begin{aligned} \mathbb{P}(\omega_n \in A^1(x^{i_1 \dots i_n}, x^{i_1 \dots i_n k}) \mid \omega_{n-1} \in A^1(x^{i_1 \dots i_{n-1}}, x^{i_1 \dots i_n}), \\ \dots, \omega_0 \in A^1(x, x^{i_1})) \\ = \mathbb{P}(\omega_n \in \{k\} \mid \omega_{n-1} \in \{i_n\}, \dots, \omega_0 \in \{i_1\}) \\ = \mathbb{P}(\omega_n = k \mid \omega_{n-1} = i_n, \dots, \omega_0 = i_1) = p_{i_n k}. \end{aligned}$$

For the right hand side we have

$$\begin{aligned} \mathbb{P}(\omega_n \in A^1(x^{i_1 \dots i_n}, x^{i_1 \dots i_n k}) \mid \omega_0 \cdot \dots \cdot \omega_{n-1} \in A^n(x, x^{i_1 \dots i_n})) \\ = \mathbb{P}(\omega_n = k \mid \omega_0 \cdot \dots \cdot \omega_{n-1} \in \{\alpha : \alpha \equiv i_1 \cdot \dots \cdot i_n \pmod{|\langle x \rangle|}\}), \end{aligned}$$

as required.  $\square$

**Lemma 5.2** Let  $|\langle x \rangle|$  be a prime number,  $S \subseteq \{1, \dots, |\langle x \rangle| - 1\}$  and let  $i_1 \cdot \dots \cdot i_n, i_r \in S$  and  $j_1 \cdot \dots \cdot j_n, j_r \in S$  be arbitrary ordered products. Then if  $i_1 \cdot \dots \cdot i_n \equiv j_1 \cdot \dots \cdot j_n \pmod{|\langle x \rangle|}$  and  $p_{i_1 i_2} \cdot \dots \cdot p_{i_{n-1} i_n} > 0$  and  $p_{j_1 j_2} \cdot \dots \cdot p_{j_{n-1} j_n} > 0$  the Markov equation (14) implies that

$$p_{i_n k} = p_{j_n k} \quad \text{for all } k \in S,$$

i.e. row  $i_n$  is equal to row  $j_n$  in the transition matrix  $P$ .

**Proof.** Let  $j$  be an arbitrary element in  $S$ . Consider the  $n+1$  step realization  $(x^{i_1}, \dots, x^{i_1 \cdot \dots \cdot i_n}, x^{i_1 \cdot \dots \cdot i_n k})$ , given that the  $n$  step realization  $(x^{i_1}, \dots, x^{i_1 \cdot \dots \cdot i_n})$  has occurred. Then from the previous lemma we have that

$$p_{i_n k} = \mathbb{P}(\omega_n = k \mid \omega_0 \cdot \dots \cdot \omega_{n-1} \in \{\alpha : \alpha \equiv i_1 \cdot \dots \cdot i_n \pmod{|\langle x \rangle|}\}). \quad (17)$$

Then consider the  $n+1$  step realization  $(x^{j_1}, \dots, x^{j_1 \cdot \dots \cdot j_n}, x^{j_1 \cdot \dots \cdot j_n k})$ , given the realization  $(x^{j_1}, \dots, x^{j_1 \cdot \dots \cdot j_n})$ . According to the previous lemma

$$p_{j_n k} = \mathbb{P}(\omega_n = k \mid \omega_0 \cdot \dots \cdot \omega_{n-1} \in \{\alpha : \alpha \equiv j_1 \cdot \dots \cdot j_n \pmod{|\langle x \rangle|}\}). \quad (18)$$

Since by hypothesis  $i_1 \cdot \dots \cdot i_n \equiv j_1 \cdot \dots \cdot j_n \pmod{|\langle x \rangle|}$ , the left hand side of (17) and (18) must coincide. Consequently,  $p_{i_n k} = p_{j_n k}$  for every  $k \in S$ , as required.  $\square$

**Lemma 5.3** Let  $\sigma$  be an arbitrary permutation on  $\mathbb{F}_{2n}$  for some natural number  $n$ . Then the map

$$\gamma_\sigma : \mathbb{F}_{2n} \rightarrow \mathbb{F}_{2n}, \quad i \mapsto i + \sigma(i),$$

is not onto.

**Proof.**<sup>7</sup> Assume the opposite. By hypothesis

$$\sum_{i=0}^{2n} i \equiv \sum_{i=0}^{2n} [i + \sigma(i)] \pmod{2n}.$$

The left hand side of this equation is  $(2n-1)n$  which is congruent to  $-n$  modulo  $2n$ . But the sum in the left hand side is twice this sum and thus congruent to 0 modulo  $2n$  contrary hypothesis.  $\square$

Note that multiplication modulo  $p$  is isomorphic to addition modulo  $p-1$  for every prime number  $p$ . Moreover  $p-1$  is even, so that have

**Corollary 5.1** Let  $\sigma$  be an arbitrary permutation on  $\mathbb{F}_p^*$ . Then the map

$$\gamma_\sigma : \mathbb{F}_p^* \rightarrow \mathbb{F}_p^*, \quad i \mapsto i\sigma(i),$$

is not onto.

---

<sup>7</sup>This proof is due to Robert Lagergren at the Department of Mathematics, Statistics and Computer Science at Växjö University.



**Theorem 5.1** *Let  $|\langle x \rangle|$  be a prime number and let  $S \subseteq \{1, \dots, |\langle x \rangle| - 1\}$ . Then at least two rows of  $P$  are equal.*

**Proof.** As we noted before each row and each column of the transition matrix  $P$  contains a positive entry. Thus  $P$  contains  $|\langle x \rangle| - 1$  positive entries,  $(p_{i\sigma(i)})_{i=1}^{|\langle x \rangle|-1}$ , for some permutation  $\sigma$ . Now Corollary 5.1 implies that  $a\sigma(a) \equiv b\sigma(b) \pmod{|\langle x \rangle|}$  for two different elements  $a$  and  $b$  in  $\mathbb{F}_p^*$ . Then, by Lemma 5.2, row  $\sigma(a)$  equals row  $\sigma(b)$ .  $\square$

**Example** Let  $|\langle x \rangle| = 5$  and  $S = \{1, 2, 3, 4\}$ . By the group property every element in  $\mathbb{F}_5^*$  can be written as a product of two elements in four ways if we do care about order:

$$\begin{aligned} 1 &= 1 \cdot 1 = 2 \cdot 3 = 3 \cdot 2 = 4 \cdot 4 \\ 2 &= 1 \cdot 2 = 2 \cdot 1 = 3 \cdot 4 = 4 \cdot 3 \\ 3 &= 1 \cdot 3 = 2 \cdot 4 = 3 \cdot 1 = 4 \cdot 2 \\ 4 &= 1 \cdot 4 = 2 \cdot 2 = 3 \cdot 3 = 4 \cdot 1. \end{aligned}$$

Then if  $p_{11}, p_{23}, p_{32}, p_{44} > 0$  we have according to Lemma 5.2 that  $p_{1k} = p_{3k} = p_{2k} = p_{4k}$  so that the rows of the transition matrix  $P$  are constant. Thus we obtain the following result.

**Theorem 5.2** *Let  $|\langle x \rangle|$  be a prime number and let  $S \subseteq \{1, \dots, |\langle x \rangle| - 1\}$ . If  $|\langle x \rangle| - 1$  entries of the transition matrix  $P$  are greater than zero and the product of the indeces for each of these entries are equal, then  $(x^{S_n})_{x \in X}$  is a Markov family if and only if  $\theta$  is a Bernoulli shift.*

Let us now study the case when  $S = \{a, b\} \subset \{1, \dots, |\langle x \rangle| - 1\}$  (and  $|\langle x \rangle|$  is a prime). Then we define the transition matrix  $P$ ,

$$P = \begin{pmatrix} p_{aa} & p_{ab} \\ p_{ba} & p_{bb} \end{pmatrix},$$

generating the Markov measure  $\mathbb{P} = \mu_{\pi P}$ . We obtain the following result

**Theorem 5.3** *Let  $|\langle x \rangle|$  be a prime number and let  $S = \{a, b\}$  be a subset of  $\{1, \dots, |\langle x \rangle| - 1\}$ . Then  $(x^{S_n})$  is a Markov process if and only if  $\theta$  is a Bernoulli shift.*

**Proof.** As stated before, it is necessary that each row and each column contains a positive entry. By Lemma 5.2 it is clear that if  $p_{ab}, p_{ba} > 0$  then  $p_{bk} = p_{ak}$  so that  $\theta$  has to be a Bernoulli shift. In the remaining cases we must have  $p_{aa}, p_{bb} > 0$ . But since  $|\langle x \rangle|$  is a prime number and  $a, b \neq 0$  we have (by the little theorem of Fermat) that  $a^{|\langle x \rangle|-1} \equiv b^{|\langle x \rangle|-1} \equiv 1 \pmod{|\langle x \rangle|}$ . Hence by Lemma 5.2 we have  $p_{ak} = p_{bk}$  so that  $\theta$  is a Bernoulli shift as required.  $\square$

### 5.1 The general case for $2 \times 2$ matrices

We now go on to study the general case when the order of  $x$  need not be an odd prime. The case when the order of  $x$  is not a prime is in general more difficult since the mappings  $\psi_{s_j} : x \mapsto x^{s_j}$  do not form a group in this case. We can, however, obtain some results for  $2 \times 2$  matrices, in other words, when the RDS is generated by two maps.

Let  $S = \{a, b\}$  for two natural numbers  $a$  and  $b$  such that they are distinct when considered as elements in  $\mathbb{F}_{|\langle x \rangle|}$ . For simplicity we first study the case when  $b = p$ . First we observe that for  $p > 2$  we have  $p^n \equiv 1 \pmod{p-1}$  for every natural number  $n$ . Moreover  $a^m p^n \equiv a^m \pmod{p-1}$ , and in fact, since  $|\langle x \rangle|$  is a divisor of  $p-1$  :

- (i)  $p^n \equiv 1 \pmod{|\langle x \rangle|}$ ,
- (ii)  $a^m p^n \equiv a^m \pmod{|\langle x \rangle|}$ .

Both (i) and (ii) are direct consequences of the rule:  $x \equiv y \pmod{n}$  implies  $cx \equiv cy \pmod{n}$  for any integer  $c$ . Let us do the following remarks.

**Remark 6** If  $p = 2$ ,  $\Gamma_p$  contains only one element, 1. Therefore every Markov shift will do. The dynamics is also trivial for  $|\langle x \rangle| = 2$ . Therefore we shall always assume that  $|\langle x \rangle| \geq 3$ . For  $a \equiv p \equiv 1 \pmod{|\langle x \rangle|}$  the dynamics is also trivial,  $x^{S_n(\omega)} = x$ , so that  $\phi$  will be the identity map on  $\Gamma_p$ . Consequently, condition (14) is valid (with probabilities which are equal to 1) for every possible  $n$  step realization. Therefore any Markov shift will imply that  $(x^{S_n})$  is a Markov process. Also for  $a$  satisfying  $a^2 \equiv a \pmod{|\langle x \rangle|}$  (implying  $a^n \equiv a \pmod{|\langle x \rangle|}$  for  $\forall n \in \mathbb{N}$ ) the sequences  $(x^{S_n})$  are Markov chains.  $\square$

Let us consider the case when  $a \not\equiv 1 \pmod{|\langle x \rangle|}$  and  $a^2 \not\equiv a \pmod{|\langle x \rangle|}$ . Then we obtain the following result.

**Lemma 5.4** *Let  $S = \{a, p\}$  where*

$$\begin{cases} a \not\equiv 1 \pmod{|\langle x \rangle|}, \\ a^2 \not\equiv a \pmod{|\langle x \rangle|}, \end{cases} \quad (19)$$

*and let  $p_{ap}, p_{pa} > 0$ . Then  $(x^{S_n})$  is a Markov process if and only if  $\theta$  is a Bernoulli shift.*

**Proof.** Suppose that  $(x^{S_n})$  is a Markov process. First note that we assume that  $p_a, p_b > 0$ . Let  $p_{pa} > 0$  and consider the realization

$$(x, x^a, x^{a^2}).$$

Then, by the condition (19), we obtain transition sets  $A^1(x, x) = \{p\}$ ,  $A^1(x, x^a) = \{a\}$  and  $A^1(x^a, x^{a^2}) = \{a\}$ . Hence the left hand side in the

Markov condition (14) is:

$$\Delta_1^3 = \mathbb{P}(\omega_2 = a \mid \omega_1 = a, \omega_0 = p) = \frac{\mathbb{P}([p, a, a])}{\mathbb{P}([p, a])} = \frac{p_p p_{pa} p_{aa}}{p_p p_{pa}} = p_{aa}.$$

For the right hand side of the Markov condition we use  $A^2(x, x^a) = \{p \cdot a, a \cdot p\}$  and obtain

$$\begin{aligned} \Delta_2^3 &= \mathbb{P}(\omega_2 = a \mid \omega_1 \cdot \omega_0 = a \cdot p) \\ &= \frac{\mathbb{P}([p, a, a]) + \mathbb{P}([a, p, a])}{\mathbb{P}([p, a]) + \mathbb{P}([a, p])} = \frac{p_p p_{pa} p_{aa} + p_a p_{ap} p_{pa}}{p_p p_{pa} + p_a p_{ap}}. \end{aligned}$$

Now, the Markov condition  $\Delta_1^3 = \Delta_2^3$  implies that

$$p_a p_{ap} p_{pa} = p_a p_{ap} p_{aa}.$$

By the condition of the lemma we conclude that  $p_{aa} = p_{pa}$ . Hence, the columns of  $P$  are constant and  $\theta$  is a Bernoulli shift.  $\square$

Note that  $p_{pa} = 0$  implies that  $p_{pp} = 1$  so that  $p$  is an absorbing state. In this case  $P$  is reducible. Also note that if  $p_{ap} = 0$  the last equality in the proof does not give any condition. Now, by the previous Lemma we obtain the following result.

**Theorem 5.4** *Let  $S = \{a, p\}$  where*

$$\begin{cases} a \not\equiv 1 \pmod{|\langle x \rangle|}, \\ a^2 \not\equiv a \pmod{|\langle x \rangle|}, \\ a^n \equiv 1 \pmod{|\langle x \rangle|}, \end{cases} \text{ for some } n \geq 2. \quad (20)$$

*Then  $(x^{S_n})$  is a Markov process if and only if  $\theta$  is a Bernoulli shift.*

**Proof.** Suppose that  $(x^{S_n})$  is a Markov process. By the previous lemma we can assume that  $p_{ap}$  or  $p_{pa}$  equals zero. Now let  $m = \min\{n : a^n \equiv 1 \pmod{|\langle x \rangle|}\}$ . Consider the following three cases:

- 1) Let  $p_{ap} > 0$  and  $p_{pa} = 0$ , so that  $p_{pp} = 1$ . Consider the  $m + 1$  step realization

$$(x, \dots, x, x^a).$$

Then by the condition of the Theorem we have transition sets  $A^1(x_i, x_{i+1}) = \{p\}$  for  $0 \leq i \leq m$  and  $A^1(x_m, x_{m+1}) = \{a\}$ . Therefore the left hand side of (14) is

$$\Delta_1^{m+1} = \frac{\mathbb{P}([p, \dots, p, a])}{\mathbb{P}([p, \dots, p])} = \frac{p_p p_{pp} \dots p_{pp} p_{pa}}{p_p p_{pp} \dots p_{pp}} = p_{pa},$$

and since  $A^m(x, x) = \{a^m, p^m\}$  the right hand side of (14) becomes

$$\begin{aligned}\Delta_2^{m+1} &= \frac{\mathbb{P}([p, \dots, p, a]) + \mathbb{P}([a, \dots, a, a])}{\mathbb{P}([p, \dots, p]) + \mathbb{P}([a, \dots, a])} \\ &= \frac{p_p p_{pp} \dots p_{pp} p_{pa} + p_a p_{aa} \dots p_{aa} p_{aa}}{p_p p_{pp} \dots p_{pp} + p_a p_{aa} \dots p_{aa}}.\end{aligned}$$

Now the Markov condition  $\Delta_1^{m+1} = \Delta_2^{m+1}$  implies that

$$p_a p_{aa} \dots p_{aa} p_{aa} = p_a p_{aa} \dots p_{aa} p_{pa}, \quad (21)$$

so that  $p_{aa} = 0$  (since  $p_{pa} = 0$ ). Thus the columns of  $P$  are constant and consequently  $\theta$  is a Bernoulli shift .

- 2) Let  $p_{ap} = p_{pa} = 0$ . Then we can consider the above given realization. Consequently (21) is not valid since  $p_{aa} > 0$  implies that the left hand side of (21) is positive while  $p_{pa} = 0$  implies that the right hand side is zero.

- 3) Let  $p_{ap} = 0$  and  $p_{pa} > 0$ , so that  $p_{aa} = 1$ . Consider the  $m + 1$  step realization

$$(x^a, x^{a^2}, \dots, x^{a^{m-1}}, x, x). \quad (22)$$

Then by the condition of the Theorem we have transition sets  $A^1(x_i, x_{i+1}) = \{a\}$  for  $0 \leq i \leq m$  and  $A^1(x_m, x_{m+1}) = \{p\}$ . Therefore the left hand side of (14) is

$$\Delta_1^{m+1} = \frac{\mathbb{P}([a, \dots, a, p])}{\mathbb{P}([a, \dots, a])} = \frac{p_a p_{aa} \dots p_{aa} p_{ap}}{p_a p_{aa} \dots p_{aa}} = p_{ap},$$

and since  $A^m(x, x) = \{a^m, p^m\}$  the right hand side of (14) becomes

$$\begin{aligned}\Delta_2^{m+1} &= \frac{\mathbb{P}([a, \dots, a, p]) + \mathbb{P}([p, \dots, p, p])}{\mathbb{P}([a, \dots, a]) + \mathbb{P}([p, \dots, p])} \\ &= \frac{p_a p_{aa} \dots p_{aa} p_{ap} + p_p p_{pp} \dots p_{pp} p_{pp}}{p_a p_{aa} \dots p_{aa} + p_p p_{pp} \dots p_{pp}}.\end{aligned}$$

Now the Markov condition  $\Delta_1^{m+1} = \Delta_2^{m+1}$  implies that

$$p_p p_{pp} \dots p_{pp} p_{pp} = p_p p_{pp} \dots p_{pp} p_{ap},$$

so that  $p_{pp} = p_{ap}$  (since  $p_{pp} > 0$ ). Thus the columns of  $P$  are constant in every case and consequently  $\theta$  is a Bernoulli shift .  $\square$

Note that  $a \equiv -1 \pmod{|\langle x \rangle|}$  is a solution to (20) for  $|\langle x \rangle| \geq 3$ . Thus we have:

**Corollary 5.2** *Let  $S = \{a, p\}$ . Then if  $a \equiv -1 \pmod{|\langle x \rangle|}$  for some  $x \in \Gamma_p$  with  $|\langle x \rangle| \geq 3$ , the dynamics on  $\Gamma_p$  is Markovian if and only if  $\theta$  is a Bernoulli shift.*

We now study the dynamics on  $\Gamma_p$  when  $S = \{a, b\}$  and  $p$  is a divisor of  $b$ . This is in fact equivalent to the case when  $b \in \mathbb{N}$  is arbitrary, since  $b = kp$ ,  $k \in \mathbb{N}$  implies that  $b^n \equiv k^n p^n \equiv k^n \pmod{|\langle x_0 \rangle|} \forall n \in \mathbb{N}$ . Hence we study  $S = \{a, b\}$ ,  $a, b \in \mathbb{N}$ .

**Remark 7** Our previous results for  $b = p$  can be generalized directly to the case when  $b \equiv 1 \pmod{|\langle x \rangle|}$ .  $\square$

For  $b = p$  we found that if  $a$  satisfies (19) and  $p_{ap}, p_{pa} > 0$ , then the Markov shift  $\theta$  has to be a Bernoulli shift. This result can be generalized according to:

**Lemma 5.5** *Let  $S = \{a, b\}$  where*

$$\begin{cases} a \not\equiv b \pmod{|\langle x \rangle|}, \\ ab \not\equiv b^2 \pmod{|\langle x \rangle|}, \\ a^2 \not\equiv ab \pmod{|\langle x \rangle|}, \\ a^2 b \not\equiv ab^2 \pmod{|\langle x \rangle|}. \end{cases} \quad (23)$$

*Then if  $p_{ab}, p_{ba} > 0$ ,  $(x^{S_n})$  is a Markov process if and only if  $\theta$  is a Bernoulli shift.*

**Proof.** Replacing  $p$  by  $b$ , and considering the realization  $(x^b, x^{ba}, x^{ba^2})$  the proof is identical to that of Lemma 5.4.  $\square$

It is clear that  $a \equiv 2 \pmod{|\langle x \rangle|}$  and  $b \equiv 1 \pmod{|\langle x \rangle|}$  are solutions of (23). The same holds for  $a \equiv -1 \pmod{|\langle x \rangle|}$ . In Appendix B we have shown that the numbers  $a \equiv -2 \pmod{|\langle x \rangle|}$  and  $b \equiv -1 \pmod{|\langle x \rangle|}$  also satisfy (23).

We may ask for the existence of more solutions. The answer is that these are the only general solutions for  $|\langle x_0 \rangle| \geq 3$ . But of course the number of solutions may far exceed the one given above even for small orders of  $\langle x \rangle$ . For  $|\langle x \rangle| = 5$  we have that every combination of  $a$  and  $b$  for which  $a \not\equiv b \pmod{|\langle x \rangle|}$ , satisfies the condition (23). Whereas for  $|\langle x \rangle| = 6$  there only exists one more solution,  $a \equiv 2 \pmod{|\langle x \rangle|}$  and  $b \equiv 4 \pmod{|\langle x \rangle|}$ , which is, however, not a solution for  $|\langle x \rangle| = 8$ .

We now give a generalization of Theorem 5.4.

**Theorem 5.5** *Let  $S = \{a, b\}$  and suppose  $(a, b)$  satisfies (23) with the additional condition*

$$a^n \equiv b^n \pmod{|\langle x \rangle|}, \quad a^{n+1} \not\equiv b^{n+1} \pmod{|\langle x \rangle|},$$

*for some  $n \geq 2$ . Then  $(x^{S_n})$  is a Markov process if and only if  $\theta$  is a Bernoulli shift.*

**Proof.** We replace  $p$  by  $b$  and replace the condition  $a^n \equiv b^n \pmod{|\langle x \rangle|}$  by  $a^n \equiv b^n \pmod{|\langle x \rangle|}$  in Theorem 5.4. Then, if we consider the realizations  $(x^b, \dots, x^{b^{m-1}}, x^{a^m}, x^{a^{m+1}})$  and  $(x^a, \dots, x^{a^{m-1}}, x^{b^m}, x^{b^{m+1}})$  respectively (for the case 1) and 3) in the proof of Theorem 5.4), the proof can be completed with the same procedure as in the proof of Theorem 5.4.  $\square$

## 6 Concluding remarks

Given a transition matrix  $P$  and a prime  $p, p \not\equiv 1 \pmod{4}$ , Lemma 5.2 was found as a useful tool for deciding whether the dynamics on  $\Gamma_p$  is Markovian or not. But this result is not just about RDS (defined on  $\Gamma_p$ ) generated by monomial mappings.

Let  $|\langle x \rangle|$  be a prime number and let  $S = \{1, \dots, |\langle x \rangle| - 1\}$ . To each  $a \in S$  there is a corresponding monomial mapping  $\psi_a : x \mapsto x^a$  and vice versa. Moreover by (16) we have

$$\psi_a \circ \psi_b x = \psi_c \circ \psi_d x \quad \Leftrightarrow \quad ab \equiv cd \pmod{|\langle x \rangle|}.$$

Hence the composition of mappings in  $(\psi_s)_{s \in S}$  is a binary operation with the same properties as multiplication in  $\mathbb{F}_{|\langle x \rangle|}^*$ . Consequently, the map

$$\gamma : \mathbb{F}_{|\langle x \rangle|}^* \rightarrow (\psi_s)_{s \in S}, \quad s \mapsto \psi_s,$$

is an (algebraic) isomorphism. In this way the  $(\psi_s)_{s \in S}$  form a group of mappings on  $\langle x \rangle \setminus \{1\}$ <sup>8</sup> isomorphic to  $\mathbb{F}_{|\langle x \rangle|}^*$ . Note that in this case the family  $(\psi_s)_{s \in S}$  is in fact a subgroup of  $\text{perm}(\langle x \rangle \setminus \{1\})$ , the group of all permutations on  $\langle x \rangle \setminus \{1\}$  (or on  $|\langle x \rangle| - 1$  letters). Therefore we can consider the RDS  $\phi$  on  $\langle x \rangle \setminus \{1\}$  as generated by a group of permutations on  $\langle x \rangle \setminus \{1\}$  (or on  $|\langle x \rangle| - 1$  letters).

We are now in a position to make some more general statements. The idea is the following. Let  $X$  be a finite state space and let the family  $\psi = (\psi_s)_{s \in S}$  of mappings be a subgroup of  $\text{perm}(X)$ <sup>9</sup> isomorphic to  $\mathbb{F}_p^*$  and let  $\theta$  be a Markov shift on  $S^{\mathbb{N}}$ . Then consider the RDS  $\varphi$  generated by  $\psi$  (in the sense of section 1.2). Define transition sets  $A^n(x, y) = \{i_1 \cdot \dots \cdot i_n : \psi_{i_n} \circ \dots \circ \psi_{i_1} x = y, \quad i_k \in S\}$ . Then a corresponding stochastic process  $(\varphi(n, \cdot)x)_{n \in \mathbb{Z}^+}$  is a Markov process if and only if the Markov equation (14) holds true. Now, with just a slight modification (not counting modulo  $|\langle x \rangle|$  but operating with the binary operation of composition on  $\text{perm}(X)$ ), we obtain a result analogous to the one in Lemma 5.2.

<sup>8</sup>Remember that the dynamics is restricted to  $\langle x \rangle \setminus \{1\}$  when  $S = \{1, \dots, |\langle x \rangle| - 1\}$  and  $|\langle x \rangle|$  is prime, see Remark 3.

<sup>9</sup>These are automatically measurable since in the finite case  $X$  is endowed with the  $\sigma$ -algebra consisting of all subsets of  $X$ .

**Lemma 5.2'** *Let  $i_1, \dots, i_n, i_r \in S$  and  $j_1, \dots, j_n, j_r \in S$  be arbitrary. Then if  $\psi_{i_n} \circ \dots \circ \psi_{i_1} x = \psi_{j_n} \circ \dots \circ \psi_{j_1} x$  and  $p_{i_1 i_2} \cdot \dots \cdot p_{i_{n-1} i_n} > 0$  and  $p_{j_1 j_2} \cdot \dots \cdot p_{j_{n-1} j_n} > 0$  the Markov equation (14) implies that*

$$p_{i_n k} = p_{j_n k} \quad \text{for all } k \in S,$$

*i.e. row  $i_n$  is equal to row  $j_n$  in the transition matrix  $P$ .*

In section 5, Theorem 5.1, we found that, requiring Markovian dynamics, at least two rows of  $P$  had to be equal. In fact we propose a much stronger version of this theorem.

**Theorem 5.1'** *Let  $|\langle x \rangle|$  be a prime number and let  $S \subseteq \{1, \dots, |\langle x \rangle| - 1\}$ . Then  $(x^{S_n})$  is a Markov family if and only if all rows of  $P$  are equal, i.e.  $\theta$  is a Bernoulli shift.*

## A Attractors

Here we give the definition of an attractor via convergens in probability which is worked out in the paper, [27], of Ochs. Let  $\varphi: \mathbb{T} \times \Omega \times X \rightarrow X$  be a RDS on the metric space  $X$  with metric  $d$ . A *random set* is a set  $B \in \mathcal{F} \otimes \mathcal{B}$  such that  $\omega \mapsto d(x, B(\omega))$  is measurable for every  $x \in X$ , where  $B(\omega)$  denotes the *section*  $B(\omega) := \{x \in X: (\omega, x) \in B\}$  and  $d(x, B(\omega)) := \inf\{d(x, y): y \in B(\omega)\}$ .  $B$  is said to be a *random compact set*, if each  $B(\omega)$  is a compact subset of  $X$ . A set  $B \subset \Omega \times X$  is a random compact set if and only if the  $B(\omega)$  are compact and  $\omega \mapsto B(\omega)$  is measurable with respect to the Borel  $\sigma$ -algebra generated by the Hausdorff distance between compact subsets of  $X$ . This metric we denote by  $\text{dist}$  so that  $\text{dist}(A, B) := \sup_{x \in A} d(x, B)$ .

**Definition (Attractor, Basin of attraction)** Let  $B \subset \Omega \times X$  be a random set. A random compact set  $A \subset B$  is called a *weak random  $B$  attractor*, if

- 1)  $A$  is strictly forward invariant, i.e.  $\varphi(t, \omega)A(\omega) = A(\theta(t)\omega)$  for every  $\omega \in \Omega$  and  $t > 0$ ,
- 2)  $A$  attracts random compact sets in probability, i.e.

$$\begin{aligned} \lim_{t \rightarrow \infty} \mathbb{P}\{\omega: \text{dist}(\varphi(t, \omega)C(\omega), A(\theta(t)\omega)) > \epsilon\} \\ = \lim_{t \rightarrow \infty} \mathbb{P}\{\text{dist}(\theta(t)C, A) > \epsilon\} = 0, \end{aligned}$$

for every random compact set  $C \subset B$  and every  $\epsilon > 0$ .

A maximal set  $B$  with the property of  $A$  being a  $B$  attractor is called the *basin of attraction* of  $A$ .

## B Solutions of congruences

We discuss the solutions to the system (23) of congruences for  $|\langle x_0 \rangle| \geq 3$ . It is clear that  $a \equiv 2 \pmod{|\langle x \rangle|}$  and  $b \equiv 1 \pmod{|\langle x \rangle|}$  are solutions of (23). The same holds for  $a \equiv -1 \pmod{|\langle x \rangle|}$ .

**Proposition B.1** *The numbers  $a \equiv -2 \pmod{|\langle x \rangle|}$  and  $b \equiv -1 \pmod{|\langle x \rangle|}$  are solutions to (23) (for  $|\langle x \rangle| \geq 3$ ).*

**Proof.** It is clear that the first condition is satisfied. The other two conditions are valid according to the considerations below.

$$(ii) \quad ab \equiv (-2)(-1) \equiv 2 \pmod{|\langle x \rangle|}$$

$$b^2 \equiv (-1)^2 \equiv 1 \pmod{|\langle x \rangle|}$$

$$(iii) \quad a^2b \equiv (-2)^2(-1) \equiv -4 \pmod{|\langle x \rangle|}$$

$$ab^2 \equiv (-2)(-1)^2 \equiv -2 \equiv |\langle x \rangle| - 2 \pmod{|\langle x \rangle|} \quad \square$$



## References

- [1] E. Beltrametti, G. Cassinelli, *Quantum mechanics and  $p$ -adic numbers*, Found. Phys. **2** (1972), pp 1-7.
- [2] Yu. Manin, *New dimensions in Geometry*, in: Lecture Notes in Mathematics 1111, Springer, New York, 1985, pp. 59-101.
- [3] I.V. Volovich, *Number theory as the ultimate physical theory*, Preprint TH.4781/87, 1987.
- [4] I.V. Volovich,  *$p$ -adic string*, Classical Quantum Gravity **4**, (1987) L83-L87.
- [5] P.G.O. Freund, M. Olson, *Non-Archimedean strings*, Phys. Lett. B **199** (1987), pp 186-190.
- [6] P.G.O. Freund, M. Olson, E. Witten, *Adelic string amplitudes*, Phys. Lett. B **199** (1987), pp 191-195.
- [7] I. Ya. Aref'eva, B. Dragovic, I.V. Volovich, *On the  $p$ -adic summability of the anharmonic oscillator* Phys. Lett. B **200** (1988), pp 512-514.
- [8] I. Ya. Aref'eva, B. Dragovic, P.H. Frampton, I.V. Volovich, *The wave function of the Universe and  $p$ -adic gravity*, Int. J. Modern Phys. A **6**(24) (1991), pp 4341-4358.
- [9] V.S. Vladimirov, I.V. Volovich, E.I. Zelenov,  *$p$ -adic Numbers in Mathematical Physics*, World Scientific, Singapore, 1994.
- [10] A. Yu. Khrennikov,  *$p$ -adic Valued Distributions in Mathematical Physics*, Kluwer Academic Publishers, Dordrecht, 1994.
- [11] S. Albeverio, W. Karwowski, *A random walk on  $p$ -adics- the generator and its spectrum*, Stochastic Process Appl. **53** (1994), pp 1-22.
- [12] A. Yu. Khrennikov,  *$p$ -adic discrete dynamical systems and collective behaviour of information states in cognitive models*. Discrete Dynamics in Nature and Society, **5**, (2000) 59-69.
- [13] A. Yu. Khrennikov, *Non-Archimedean Analysis: Quantum Paradoxes, Dynamical Systems and Biological Models*, Kluwer Academic Publishers, Dordrecht, 1997.
- [14] A. Yu. Khrennikov, *On the problem of small denominators in the field of complex  $p$ -adic numbers*. Reports from Växjö University - Mathematics, natural sciences and technology, N.9, 2000.

- [15] A. H. Bikulov, I. V. Volovich, *p*-adic brownian motion. Izvestia Akademii Nauk, ser. Matematika, **61** (1999), No. 3, 75-90.
- [16] A. Yu. Khrennikov, *Human subconscious as the p-adic dynamical system*, J. theor. Biol. **193**, (1998) 179-176.
- [17] D. Dubischar, V.M. Gundlach, A. Yu. Khrennikov, O. Steinkamp, *Attractors of random dynamical systems over p-adic numbers and a model of noisy thinking*, Physica D, **130** (1999), 1-12.
- [18] S. Albeverio, A Yu. Khrennikov, B. Tirozzi, *P-adic Neural Networks*, Mathematical models and methods in applied sciences, **9** (1999) N. 9, 1417-1437.
- [19] S. Albeverio, A Yu. Khrennikov, P. Kloeden, *Memory retrieval as a p-adic dynamical system*, BioSystems, **49** (1999), 105-115.
- [20] L. Arnold, *Random Dynamical Systems*, Springer-Verlag, 1997.
- [21] E.B. Dynkin, *Markov Processes*, Springer-Verlag, 1965.
- [22] F.Q. Gouvêa, *p-adic numbers-an introduction*, Springer-Verlag, 1997 (2 ed).
- [23] W.H. Schikhof, *Ultrametric calculus*, Cambridge University press, 1984.
- [24] P.R. Halmos, *Lectures on ergodic theory*, Kenkyusha Printing Co., Tokyo, 1956.
- [25] H.O. Peitgen, H. Jürgens, D. Saupe, *Chaos and Fractals*, New Frontiers of Science, Springer-Verlag, New York, 1992.
- [26] K.O. Lindahl, *On Markovian properties of the dynamics on attractors of random dynamical systems over p-adic numbers*, Reports from Växjö University - Mathematics, natural sciences and technology, 1999.
- [27] G. Ochs, *Probabilistic attractors*, in preparation, Institute of Dynamical Systems, Universität Bremen, 1999.